Microsoft 365 Review Report

Project	SAMPLE - Microsoft 365 Review	Reference	
Publication Date		Version	1.0 Release

Limitations

As with all security reviews, this work has been performed using information and tools currently available from national and international security organisations.

The results represent a snapshot of the environment as it was at the time of the review. It is incumbent upon the organisation to ensure that the site is kept up to date with intrusion control methods.

Kaon Security Limited, its Directors and staff cannot be held liable for any losses, direct or consequential which may result from actioning, or not actioning, recommendations provided in the report.

Confidentiality

The data gathered during this process will be used for the purposes of this review only.

All information gathered on site is stored on an encrypted hard drive.

All information gathered during the review and reports generated, with the exception of the executive and technical summaries, will be wiped from Kaon Security's information systems upon acceptance of the report by you.

Any output produced by Kaon Security (and all the information within) is strictly for the eyes of SAMPLE staff members and senior management only. In the event where any part of the information is required to be shared with any 3rd party, sister organisation, or vendor, Kaon Security's written approval is required.

Table of Contents

Executive Summary

SAMPLE appointed Kaon Security (KS) to perform a security review of the current Microsoft 365 setup.

A detailed scope is defined within the section titled *Scope*.

Kaon Security performed a remote interview of a nominated SAMPLE staff member…

Microsoft 365 Review

Kaon Security found that the Microsoft 365 environment at SAMPLE is well configured in many areas. We did however find many critical and high risk security issues, and numerous opportunities for improvement.

The following table illustrates the high level findings across the Microsoft 365 environment.

Please note: Numbers in this table are not representative – example purposes only

M365 Review Outcome					
Configuration Section	**Critical**	**High**	**Medium**	**Low**	**Total**
M365	1	1	1	1	4
Azure Active Directory (AAD)	2	2	2	2	8
Endpoint Manager	3	3	3	3	12
Exchange Admin	4	4	4	4	16
OneDrive	5	5	5	5	20
Security	6	6	6	6	24
Compliance	7	7	7	7	28
SharePoint	8	8	8	8	32
Power Apps	9	9	9	9	36
Dynamics 365	10	10	10	10	40
Cloud App Security	11	11	11	11	44
Power Automate	12	12	12	12	48
Teams	13	13	13	13	52
Other	14	14	14	14	56

Recommendations for Security Posture

Kaon Security provides these recommendations based on the limited information collected during a passive interview. We therefore advise taking these as guidelines only.

Kaon Security believes that the following additional security considerations would benefit SAMPLE by integrating security, monitoring, intelligence, and incident response components. Furthermore, end to end security integration would help to train and prepare SAMPLE for future security activities.

1. Document a well-defined ICT Data Governance security policy.
2. Data discovery, identification, classification, and sensitive data registry.

Please note: Recommendations for Security Posture can vary from site to site, can be up to 15 recommendations.

Key Observations and Recommendations

This section provides key observations and relevant recommendations.

Microsoft 365 Review

Kaon Security performed a detailed review of the current configurations of Microsoft 365 and Microsoft 365 specific items within Azure Active Directory for SAMPLE and found the following issues:

1. SAMPLE infrastructure allows users to join any new device to their Microsoft 365 account without a defined approval process. In the case of a compromised account, an attacker would have easy access to register rogue devices.
2. The Microsoft 365 online configuration allows third-party storage systems to be used for sharing and viewing content. It is unusual to allow this inter-cloud functionality because Microsoft 365 provides 1TB of OneDrive secure storage at no additional cost.

Please note: Microsoft 365 Review content varies from site to site, can be up to 25 findings

Additional Recommendations

Kaon Security identified the following key summarised recommendations:

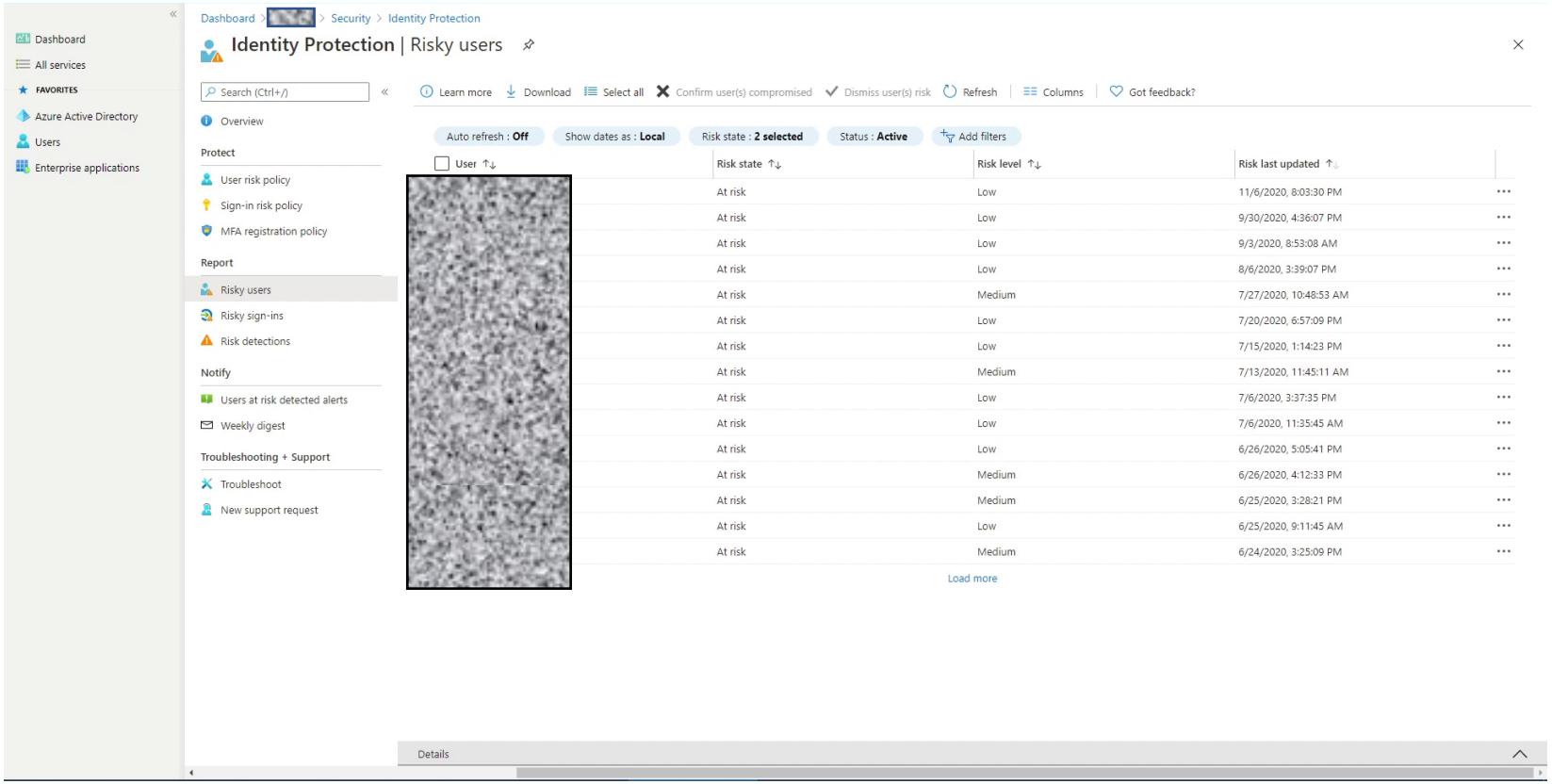
1. A detailed fine tuning of the Microsoft 365 configurations as per the *Key Findings* section.
2. Perform a Cloud exposure mapping activity to identify all other SaaS solutions used across the SAMPLE IT infrastructure.

Please note: Additional Recommendations varies from site to site, can be between 10 to 20 recommendations.

Key Findings

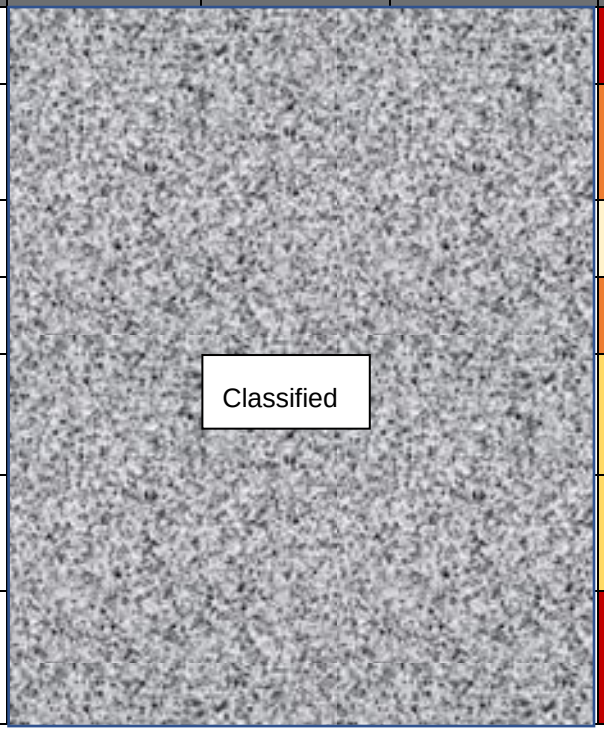
Urgent Attention Required

This section looks through some of the items in urgent need of review or analysis. We consider these items to potentially be active risks and recommend attending to them ASAP. Refer finding number 49 in *All Issues Found* table.



All Issues Found

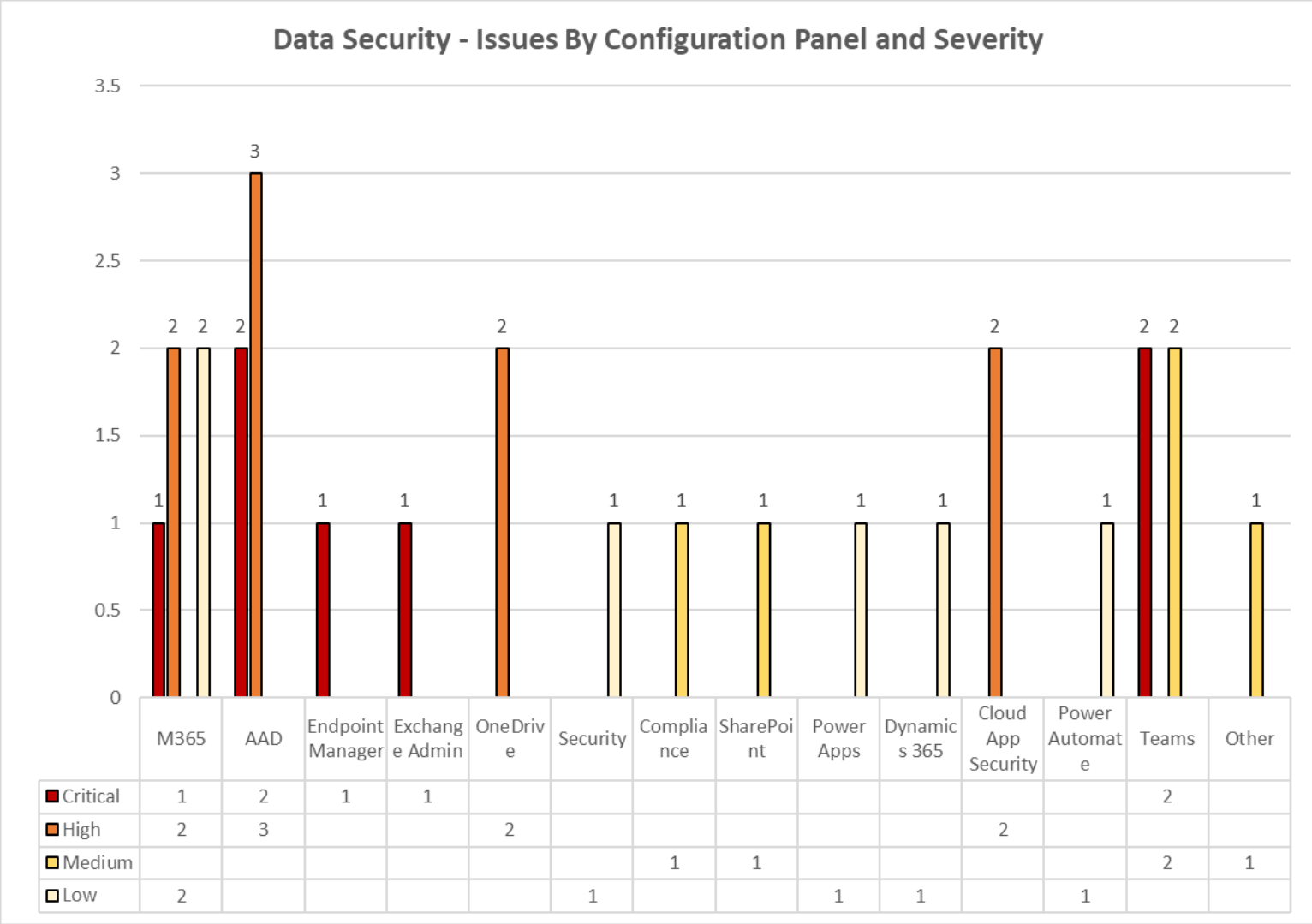
Kaon Security categorised multiple issues based on their risk type; the following table lists all the issues found during this activity.

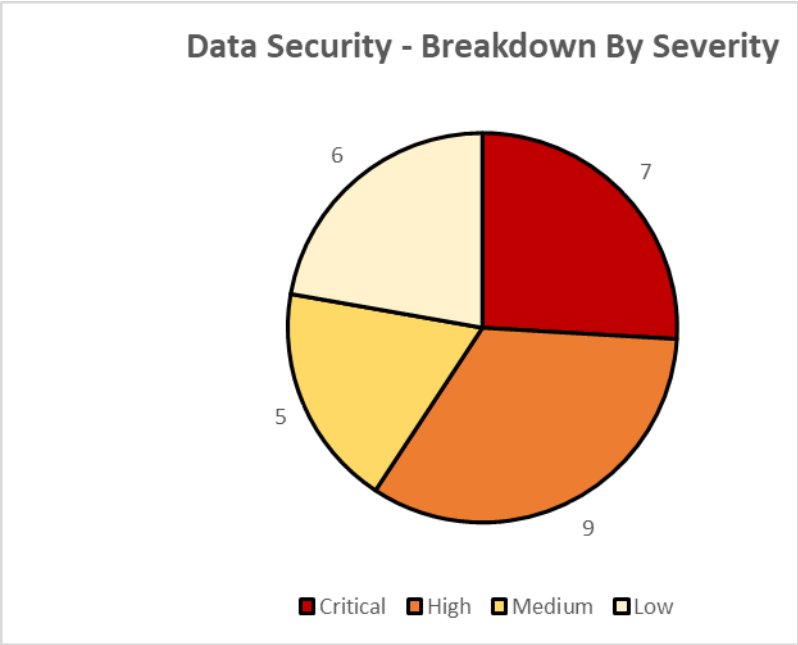
Microsoft 365 Configuration Review										
Sr. No	Configuration Panel	Configuration Item	Description	Current Value	Recommended Value	Severity	Complexity	Time to Achieve	Security Impact	Issue Type
1	M365	Users				***Critical***	Easy	5 Min	High	Security Exposure
2	M365	Domains				**High**	Easy	1 Hour	High	Misconfiguration
23	AAD	Password Reset				**Low**	Easy	TBC	Medium	None
46	AAD	Password Reset				**High**	Easy	5 Min	High	Data Security
65	Compliance	Improvement Actions				**Medium**	High	TBC	High	Data Security
73	Compliance	Data Classification				**Medium**	Medium	TBC	High	Data Security
84	Endpoint Manager	Noncompliant Devices				***Critical***	Easy	1 hour	High	Data Security

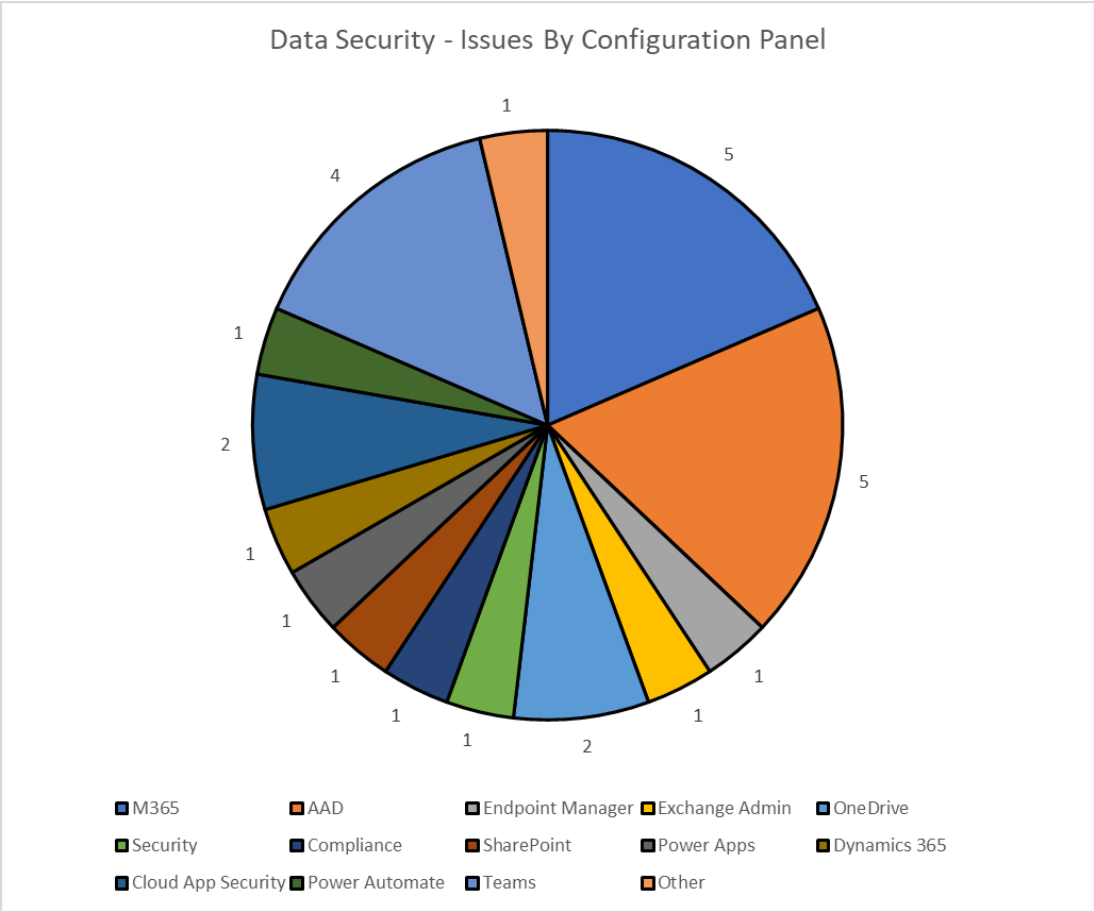
Please note: content of table varies from site to site, can be between 60 to 100 entries!

Data Security Issues

Kaon Security categorised multiple issues based on their risk type; the following issues are identified as Data Security.




Data Security - Breakdown By Severity
7
9
5
6
Critical
High
Medium
Low


Data Security - Issues By Configuration Panel
5
5
1
1
2
1
1
1
1
1
1
2
1
4
1
M365
AAD
Endpoint Manager
Exchange Admin
OneDrive
Security
Compliance
SharePoint
Power Apps
Dynamics 365
Cloud App Security
Power Automate
Teams
Other

Security Exposure Issues

Kaon Security categorised multiple issues based on their risk type; the following issues are identified as Security Exposure.

Please note: Additional graphs will be provided for Security Exposure Issues

Privacy Issues

Kaon Security categorised multiple issues based on their risk type; the following issues are identified as Privacy.

Please note: Additional graphs will be provided for Privacy Issues

Misconfiguration Issues

Kaon Security categorised multiple issues based on their risk type; the following issues are identified as Misconfiguration.

Please note: Additional graphs will be provided for Misconfiguration Issues

Other Issues

Kaon Security categorised multiple issues based on their risk type; the following issues are identified as Other.

Please note: Additional graphs will be provided for Other Issues